AUTHENTICATION AND DATA SECURITY SYSTEM FOR COMMUNICATIONS

CLAIMS

I claim:

1. An authentication and data security system for communications in which

a) a communication key is derived by a first party subsystem using an encryption algorithm from key data previously provided by a second party subsystem to the first party subsystem;

b) the communication key is transmitted to the second party subsystem, which uses a decryption algorithm to check whether the communication key was derived from any of various key data from a previously provided data pool related to the first party subsystem;

2. The authentication and data security system of Claim 1, in which the communication key is transmitted to a third party subsystem, which uses the communication key without decryption as an authentication key in communications with the first and second parties regarding for a specific transaction involving the three parties.

3. The authentication and data security system of Claim 2, in which the second party subsystem processes a request to approve the transaction from the third party subsystem if the communication key was derived from any of various key data from the previously provided data

pool related to the first party subsystem;

4. The authentication and data security system of Claim 3, in which the second party subsystem transmits the results of the request to approve, to the third party subsystem.

5. The authentication and data security system of Claim 4, in which the second party subsystem confirms its approval of the transaction by seeking an approval from the first party subsystem, prior to transmitting the second party subsystem's approval to the third party subsystem.

6. The authentication and data security system of Claim 2, in which the first and second parties are privy to the key data, but it is not revealed to the third party subsystem.

7. The authentication and data security system of Claim 2, in which the first party subsystem is within a consumer's system, the second party subsystem is within a financial institution's system, the third party subsystem is within a merchant's system, and the key data is credit card data.

8. The authentication and data security system of Claim 2, in which the communication key but not the credit card data is transmitted by the first party subsystem over the internet to the second party subsystem, who in turn transmits it with a request to authorize the transaction to the third party subsystem.

9. The authentication and data security system of Claim 1, in which the encryption algorithm is

dynamic.

10. The authentication and data security system of Claim 9, in which the encryption algorithm is a context dependent dynamic cryptosystem.

11. The authentication and data security system of Claim 10, in which the encryption algorithm includes the operations of:

a) selecting secret key p, derived from the context, being a prime number greater then 2;

b) selecting secret key n, derived from the context, being a positive integer greater then 0;

c) selecting modulus m, being a positive integer, $m = p^n$;

d) selecting an encryption key α, derived from the context, which is a member of the finite group M_m of residue classes prime to m under multiplication modulo m, and being prime to $\theta(m)$, where $\theta(m) = p^n(1 - 1/p)$;

e) selecting a communication key $\alpha 1$, which is a member of the finite group M_m of residue classes prime to m under multiplication modulo m, and being prime to $\theta(m)$, where $\alpha 1$ can be determined using $\alpha * \alpha 1 \equiv 1 \bmod \theta(m)$.

12. The authentication and data security system of Claim 11, in which the decryption algorithm

includes processing the communication key as a member of Z_m whereby the operations can be determined using $\alpha^*\alpha 1 \equiv 1 \bmod \theta(m)$.

13. The authentication and data security system of Claim 11, in which the encryption algorithm includes credit card information as the context.

14. The authentication and data security system of Claim 11, in which the encryption algorithm includes a unique context parameter that varies the communication key for each communication session, the key data being thereby indeterminable by an outside party subsystem who might monitor a series of such communication keys.

15. The authentication and data security system of Claim 11, in which the encryption algorithm includes a parameter from a context that is continually changing, by which the communication key varies for each communication session, the key data being thereby indeterminable by an outside party subsystem who might monitor a series of such communication keys.

16. The authentication and data security system of Claim 15, in which the parameter is selected at a time known only to the parties intended to decrypt the communication key.

17. The authentication and data security system of Claim 1, in which the communication key for a specific communication session is derived from the key data in combination with a parameter based on an incremented number related to the current communication session in a series of communications between the first and second parties.

18. The authentication and data security system of Claim 17, in which the parameter is the number of the current communication session in a series of communications between the first and second parties, and the number is stored as incremental data by each of the first and second parties to enable successive authentication and communication sessions.

19. The authentication and data security system of Claim 17, in which the parameter is a date and time relating to the current communication session,

20. The authentication and data security system of Claim 4, in which

a) the second party subsystem transmits the results of the request to approve, to the third party subsystem;

b) the second party subsystem confirms its approval of the transaction by seeking an approval from the first party subsystem, prior to transmitting the second party subsystem's approval to the third party subsystem;

c) the first and second parties are privy to the key data, but it is not revealed to the third party subsystem;

d) the first party subsystem is within a consumer's system, the second party subsystem is within a financial institution's system, the third party subsystem is within a merchant's system, and the

key data is credit card data;

e) the communication key but not the credit card data is transmitted by the first party subsystem over internet to the second party subsystem, which in turn transmits it with a request to authorize the transaction to the third party subsystem;

f) the encryption algorithm system is asymmetric and dynamic;

g) the encryption algorithm is a context dependent dynamic cryptosystem;

21. The authentication and data security system of Claim 20, in which the encryption algorithm includes the operations of:

a) selecting secret key p, derived from the context, being a prime number greater then 2,

b) selecting secret key n, derived from the context, being a positive integer greater then 0,

c) selecting modulus m, being a positive integer, $m = p^n$,

d) selecting an encryption key α, derived from the context, which is a member of the finite group M_m of residue classes prime to m under multiplication modulo m, and being prime to $\theta(m)$, where $\theta(m) = p^n(1 - 1/p)$;

e) selecting a communication key $\alpha 1$, which is a member of the finite group M_m of residue classes prime to m under multiplication modulo m, and being prime to $\theta(m)$, where $\alpha 1$ can be determined using $\alpha * \alpha 1 \equiv 1 \bmod \theta(m)$.

22. The authentication and data security system of Claim 21, in which the decryption algorithm includes processing the communication key as a member of Z_m whereby the operations can be determined using $\alpha * \alpha 1 \equiv 1 \bmod \theta(m)$.

23. The authentication and data security system of Claim 22, in which the encryption algorithm includes a unique context parameter that varies the communication key for each communication session, the key data being thereby indeterminable by an outside party subsystem who might monitor a series of such communication keys, the parameter being derived from the date and time of each such communication session and a number of the current communication session in a series of communications between the first and second parties, and the number is stored as incremental data by each of the first and second parties to enable successive authentication and communication sessions.

24. The authentication and data security system of Claim 1, 11, or 17, in which the first party subsystem is within a cellular phone and the second party subsystem is within a cellular phone company's system.